CLAIMS

1. A network address translating gateway connecting a LAN to an external network, said LAN using local IP addresses, said gateway having a local IP address that can be seen by devices on said LAN and having an external IP address that can be seen by devices on said external network, said gateway comprising

a plurality of internal tables associating combinations of local IP addresses of local devices on said LAN, external IP addresses of external devices on said external network, SPI-In values, SPI-Out values, source port addresses, destination port addresses, reserved port addresses, and maintaining a list of reserved port addresses,

means for performing normal address translation upon datagrams passing from said LAN to said external network and datagrams passing from said external network to said LAN,

means for delivering a datagram from a local device on said LAN to an external device on said external network by receiving a datagram from a local device on said LAN intended for delivery to an external device on said external network, and determining whether said datagram is encrypted and, if said datagram is encrypted, for determining whether the SPI of said datagram is recorded in the SPI-Out field in said internal table and, if said SPI is recorded in said SPI-Out field, modifying the source IP address of said datagram to be said external IP address of said gateway and passing said datagram to said external network for routing and delivery to said external device,

and if said SPI is not recorded in said SPI-Out field of said internal table, setting the SPI-In field corresponding to the local IP address of said local device equal to zero and setting said SPI-Out field equal to said SPI, modifying said source IP address of said

datagram to be said external IP address of said gateway and passing said datagram to said external network for routing and delivery to said external device,

and if said datagram is not encrypted, determining whether the destination port address for said datagram is included in said list of reserved port addresses and, if said destination port address is not included in said list of reserved port addresses, performing normal address translation upon said datagram and passing said datagram to said external network for routing and delivery to said external device,

and if said destination port address is included in said list of reserved port addresses, determining whether said destination port address is bound to said local IP address of said local device, and if said destination port address is bound to said local IP address, performing normal address translation upon said datagram and passing said datagram to said external network for routing and delivery to said external device,

and if said destination port address is not bound to said local IP address of said local device, modifying said source IP address of said datagram to be said external IP address of said gateway, binding said destination port address to said local IP address of said local device and creating an association between said destination port address and the external IP address of said external device, and passing said datagram to said external network for routing and delivery to said external device,

means for delivering a datagram from said external device to said local device by receiving a datagram from said external device on said external network intended for delivery to said local device on said LAN,

determining whether said datagram is encrypted and, if said datagram is encrypted, determining whether the datagram's SPI is recorded in said SPI-In field of said internal

table and, if said SPI is recorded in said SPI-In field, modifying the destination IP address of said datagram to be said local IP address of said local device and passing said datagram to said LAN for routing and delivery to said local device,

and if said SPI is not recorded in said SPI-In field of said internal table, determining whether said SPI-In field corresponding to said IP address of said external device is equal to zero and, if said SPI-In field is not equal to zero, discarding said datagram,

and if said SPI-In field is equal to zero, setting said SPI-In field equal to said SPI, modifying the destination IP address of said datagram to be said local IP address of said local device and passing said datagram to said LAN for delivery to said local device,

and if said datagram is not encrypted, determining whether the destination port address for said datagram is included in said list of reserved port addresses and, if said destination port address is not included in said list of reserved port addresses, performing normal address translation upon said datagram and passing said datagram to said LAN for delivery to said local device,

and if said destination port address is included in said list of reserved port addresses, determining whether said destination port address is bound to the local IP address of said local device, if said destination port address is not bound to said local IP address, discarding said datagram,

and if said destination port address is bound to said local IP address, modifying said destination IP address of said datagram to be said local IP address of said local device, unbinding said destination port address from said local IP address, and passing said datagram to said LAN for delivery to said local device.

2. The network address translating gateway of claim 1, further comprising a timer, wherein, upon receiving a signal that a port address has become bound to an IP address, said timer will commence timing for a predetermined length of time and, upon the expiration of said predetermined length of time, will send a signal causing said port address to become unbound from said IP address, and, upon receiving a signal indicating that said port address has become unbound from said IP address prior to the expiration of said predetermined length of time, said timer will stop timing and will reset.

3. The network address translating gateway of claim 1 in which said external network is the internet.

4. The network address translating gateway of claim 3 in which said LAN is a virtual private network.

5. A method of processing IP datagrams from a local device on a LAN using local IP addresses through a network translating gateway to an external device on an external network comprising the steps of

maintaining a plurality of tables associating local IP addresses of local devices on said LAN, external IP addresses of external devices on said external network, port addresses of said local devices, port addresses of said external devices, SPI-in values, SPI-out values, and reserved port addresses, and a list of reserved port addresses,

receiving a datagram from said LAN

determining whether said datagram is encrypted and, if said datagram is encrypted, determining whether the SPI in said datagram is recorded in the SPI-out field of one of said plurality of internal tables and, if said SPI is recorded in said SPI-out field of said internal table, modifying the source IP address to be the external IP address of said gateway and

passing said datagram to said external network for routing and delivery to said external device,

and if said SPI is not recorded in said SPI-out field of said internal table, setting said SPI-out field corresponding to the IP address of said external device equal to said SPI and setting the SPI-in field of said internal table to zero, modifying said source IP address to be said external IP address of said gateway, and passing said datagram to said external network for routing and delivery to said external device,

and if said datagram is not encrypted, determining whether the destination port address for said datagram is included in said table of reserved port addresses and, if said destination port address is not included in said table of reserved port addresses, performing normal address translation upon said datagram and passing said datagram to said external network for routing and delivery to said external device,

and if said destination port address is included in said table of reserved port addresses, determining whether said destination port address is bound to an IP address, and if said destination port is bound to an IP address, performing normal address translation upon said datagram and passing said datagram to said external network for routing and delivery to said external device,

and if said destination port address is not bound to an IP address, modifying said source IP address to be said external IP address for said external device, binding said destination port address to the local IP address of said local device and creating an association between said destination port address and said external IP address of said external device, and passing said datagram to said external network for routing and delivery to said external device.

6. A method of processing IP datagrams from an external device on an external network through a network translating gateway to a local device on a LAN using local IP addresses, comprising the steps of

maintaining a plurality of tables associating local IP addresses of local devices on said LAN, external IP addresses of external devices on said external network, port addresses of said local devices, port addresses of said external devices, SPI-in values, SPI-out values, and reserved port addresses, and a list of reserved port addresses,

receiving a datagram from said external network,

determining whether said datagram is encrypted and, if said datagram is encrypted, determining whether the SPI in said datagram is recorded in the SPI-in field of one of said plurality of internal tables and, if said SPI is recorded in said SPI-in field of said internal table, modifying the destination IP address to be the internal IP address of said local device and passing said datagram to said LAN for routing and delivery to said local device,

and if said SPI is not recorded in said SPI-in field of said internal table, determining whether said SPI-in field corresponding to the IP address of said external device is zero, and if said SPI-in field is not zero, discarding said datagram,

and if said SPI-in field is equal to zero, modifying said SPI-in field to be said SPI, modifying said destination IP address to be said local IP address of said local device, and passing said datagram to said LAN for routing and delivery to said local device,

and if said datagram is not encrypted, determining whether the destination port address for said datagram is included in said list of reserved port addresses, and if said destination port address is not included in said list of reserved port addresses, performing

normal address translation and passing said datagram to said LAN for routing and delivery to said local device,

and if said destination port address is included in said list of reserved port addresses, determining whether said destination port address is bound to said local IP address, and if said destination port is not bound to said local IP address, discarding said datagram,

and if said destination port address is bound to said local IP address, modifying said destination IP address to be said local IP address of said local device, unbinding said destination port address from said local IP address, and passing said datagram to said LAN for routing and delivery to said local device.

7. The method of processing IP datagrams as claimed in claim 5, further comprising the steps of starting a timer whenever said destination port address becomes bound to said local IP address of said local device,

resettling said timer whenever said destination port address has become released,

and sending a signal whenever said timer is active and a predetermined length of time has expired from the time said timer was started.

8. The method of processing IP datagrams as claimed in claim 6, further comprising the steps of starting a timer whenever said destination port address becomes bound to said local IP address of said local device,

resettling said timer whenever said destination port address has become released,

and sending a signal whenever said timer is active and a predetermined length of time has expired from the time said timer was started.

9. The method of processing IP datagrams as claimed in claim 5, in which said external network is the internet.

10. The method of processing IP datagrams as claimed in claim 6, in which said external network is the internet.

11. The method of processing IP datagrams as claimed in claim 5 in which said LAN is a virtual private network.

12. The method of processing IP datagrams as claimed in claim 6 in which said LAN is a virtual private network.